

Dépannez les alertes de sécurité de Javas CAD

Contenu

[Introduction](#)

[Informations générales](#)

[Problème](#)

[Conditions](#)

[Solution](#)

[Alertes de sécurité](#)

[Versions UCCX avant la version 9.0\(2\)SU1](#)

[Version 9.0\(2\)SU1 UCCX](#)

[Version 10.0\(1\) UCCX](#)

[Se connecter d'email d'agent](#)

Introduction

Ce document décrit comment dépanner des alertes de sécurité de Javas sur l'email d'agent du Cisco Agent Desktop du Cisco Unified Contact Center Express (UCCX) (CAD), aussi bien que sur l'Édition navigateur de Cisco Agent Desktop (CAD-BE).

[Informations générales](#)

L'email d'agent UCCX CAD et les CAD-BE se fondent sur Javas (et applet Java) afin de fonctionner.

Les changements des règles et de l'architecture de sécurité de Javas dans les versions de Javas qui sont prises en charge par certains de l'email d'agent UCCX CAD et de versions CAD-BE produisent des alertes de sécurité accessibles à l'utilisateur ou font fonctionner les caractéristiques incorrectement ou pas du tout.

Problème

Quand vous exécutez l'email d'agent ou le CAD-BE dans un navigateur, vous recevez une nouvelle alerte de sécurité qui ressemble à ceci :

Quand vous cliquez sur **plus de lien de l'information...**, ce message apparaît :

Si vous choisissez l'option de **bloc**, l'application ne fonctionne pas correctement (ou une panne

complète de l'application se produit), et le navigateur entier pourrait se bloquer. Même si vous choisissez **ne bloquez pas** et option, Javas ne limite pas des exécutions et pourrait toujours entraîner les questions d'exécution.

Conditions

Les dernières releases de Javas traitent la transmission de Javascript-à-applet en tant que code *non signé*. Ceci fait avoir le CAD applet Java signé/non signé mélangé, qui crée une alerte de sécurité où vous êtes requis de choisir le bloc ou de débloquer l'option. Ceci affecte n'importe quel applet Java signé où il y a transmission de Javascript-à-applet.

Ces releases de Javas ont la modification mentionnée ci-dessus :

- Version 1.7.0 de Javas, mises à jour 21 et plus tard
- Version 1.6.0 de Javas, mises à jour 45 et plus tard

Note: Le CAD utilise Java Runtime Environment (JRE) pour l'email d'agent, le Cisco Supervisor Desktop (CSD), et le CAD-BE.

Solution

Cette section décrit des contournements possibles pour le problème qui est décrit dans la section précédente.

Alertes de sécurité

Cette section décrit comment dépanner des avertissements instantanés de Sécurité pour chaque version UCCX.

Versions UCCX avant la version 9.0(2)SU1

Les versions UCCX avant la version 9.0(2)SU1 prennent en charge seulement des versions de Javas jusqu'à la version 1.6.0, mise à jour 31, ainsi les installations qui exécutent actuellement les versions affectées de Javas utilisent une version sans support de Javas.

Contournement cette question, vous pouvez désinstaller Javas de l'ordinateur complètement. Quand vous vous connectez dans le CAD, le CSD, ou le CAD-BE, la bonne version de Javas sera alors installée. Après que la version Java prise en charge soit installée, les avertissements instantanés de Sécurité ne devraient pas apparaître.

Note: Si un ordinateur est directement mis à jour aux plus défuntés versions Java (sans Java désinstallez), les questions instantanées pourraient encore se produire, et l'email d'agent ne pourrait pas fonctionner comme prévu.

Version 9.0(2)SU1 UCCX

La version 9.0(2)SU1 UCCX prend en charge la version 1.6.0 de Javas, mise à jour 45 et contient la difficulté pour l'ID de bogue Cisco [CSCug80029](#).

Aucun avertissement instantané de Sécurité ne devrait apparaître, si le PC exécute la version 1.6.0 de Javas, mise à jour 45, et email d'agent fonctionne normalement.

Version 10.0(1) UCCX

La version 10.0(1) UCCX prend en charge la version 1.7.0 de Javas, mise à jour 45. Récemment, la version 1.7.0 de Javas, mise à jour 51 a été libérée. À ce moment-là, Oracle a augmenté la spécification de base de Sécurité à la mise à jour 51, qui est partie de la mise à jour 45 classée par catégorie comme *non sécurisée*. Si vous vous exécutez la version 10.0(1) UCCX et la version 1.7.0 de Javas, mise à jour 45, un avertissement instantané de Sécurité apparaît quand vous vous connectez dans l'email d'agent.

Contournement cette question, vous devez diminuer le curseur de Sécurité au **support** chez le navigateur et le clic **ne bloquent pas** chaque fois que vous recevez le message de sorte que l'email d'agent fonctionne correctement. Vous pouvez également améliorer à la version 1.7.0 de Javas, mise à jour 51 afin de résoudre ce problème. La difficulté qui est décrite dans l'ID [JDK-8027405 de](#) bogue d'Oracle, qui est inclus dans la mise à jour 51, devrait empêcher de futures occurrences de cette question.

Conseil : Référez-vous à l'ID de bogue Cisco [CSCum69044](#) pour information les informations complémentaires.

Se connecter d'email d'agent

Après version 1.7.0 de Javas, la mise à jour 45 a été intégrée dans le CAD pour la version 10.0 UCCX, la question décrite dans l'ID de bogue Cisco [CSCum00334](#) était due trouvé aux changements du JRE d'Oracle. Ceci a créé une question où le côté client d'email d'agent se connectant (**EEMUi*.log**) est désactivé par défaut.

Voici un résumé de la question :

- Dans la release 7u21, le JRE a exigé de l'utilisation d'un attribut manifeste de Faire confiance-*bibliothèque* afin d'empêcher l'occurrence des avertissements de popup de Sécurité. Le développement interne CAD a avec succès utilisé cet attribut afin d'atténuer la question.
- Dans la release 7u45, l'utilisation également exigée JRE d'un Appelant-*permis-Codebase* manifestent l'attribut afin d'empêcher l'occurrence d'un nouvel avertissement de popup de Sécurité.
- Les bogues JDK d'Oracle décrivent une question où la release 7u45 JRE ne permet pas la Faire confiance-*bibliothèque* et Appelant-*permis-Codebase* manifestez les attributs pour coexister. S'ils font, le dernier attribut est ignoré.

- Le contournement d'Oracle était d'utiliser seulement l'Appelant-*permis-Codebase* manifestent l'attribut, qui devrait avoir empêché l'occurrence des deux avertissements de popup de Sécurité. Cependant, quand ce contournement est mis en application, l'avertissement instantané de la première Sécurité est déclenché pour **EemUi** quand vous tentez d'accéder aux fichiers manifestes **.jar**, qui sont exigés afin d'initialiser le sous-système se connectant.

Conseil : Référez-vous au [groupe de plate-forme Java, blog de gestion du produit](#) pour une description plus détaillée de cette question.

Oracle a dépisté cette question dans l'ID [JDK-8026347 de](#) bogue avec des plans pour le résoudre.

Note: Cette bogue est un doublon pour l'ID [JDK-8026228 de](#) bogue ; cependant, cette bogue n'est pas publiquement visualisable sans enregistrement approprié.

Quand l'ID **JDK-8026228 de** bogue est réparé, il devrait permettre au CAD d'utiliser la Faire confiance-*bibliothèque* et Appelant-*permis-Codebase* manifestez les attributs simultanément, qui devraient empêcher l'avertissement instantané de la première Sécurité quand le sous-système se connectant est utilisé (puisque cet avertissement instantané de Sécurité a été avec succès atténué en plus de l'attribut manifeste de Faire confiance-*bibliothèque* pour la version 7u21 JRE).

Conseil : Si la version 10.0 UCCX est utilisée avec l'email d'agent CAD et élimination des imperfections de côté client est prié, référez-vous à l'ID de bogue Cisco [CSCum00334](#).